BOISE MATTHEWS DONEGAN LLP
Bridget M. Donegan, OSB No. 103753
805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

Attorneys for Plaintiff Loujain Hathloul Alhathloul

FOLEY HOAG LLP
Christopher E. Hart, MA BBO No. 625031
chart@foleyhoag.com
Anthony D. Mirenda, MA BBO No. 550587
adm@foleyhoag.com
Andrew Loewenstein, MA BBO No. 648074
aloewenstein@foleyhoag.com
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1232

Attorneys for Plaintiff Loujain Hathloul Alhathloul

ELECTRONIC FRONTIER FOUNDATION
David Greene, CA Bar No. 160107
davidg@eff.org
Sophia Cope, CA Bar No. 233428
sophia@eff.org
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Attorneys for Plaintiff Loujain Hathloul Alhathloul

CENTER FOR JUSTICE AND ACCOUNTABILITY
Daniel McLaughlin, CA Bar No. 315326
dmclaughlin@cja.org
Claret Vargas, MA BBO No. 679565
cvargas@cja.org
Carmen Cheung Ka Man, NY Bar No. 4132882
ccheung@cja.org
268 Bush St. #3432
San Francisco, CA 94104
(415) 544-0444

Attorneys for Plaintiff Loujain Hathloul Alhathloul

Table of Contents

Table of Authorities

Cases

Statutes

Rules

Other Authorities

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

LOUJAIN HATHLOUL ALHATHLOUL, *Plaintiff,* v. DARKMATTER GROUP, MARC BAIER, RYAN ADAMS, and DANIEL GERICKE *Defendants.*	Civil No. 3:21-cv-01787-IM **PLAINTIFF'S OPPOSITION TO MOTION TO DISMISS AND MEMORANDUM OF LAW IN SUPPORT** **REQUEST FOR ORAL ARGUMENT**

INTRODUCTION

Loujain Alhathloul is a preeminent Saudi human rights advocate and leader in the movement to promote the rights of women and girls in Saudi Arabia. She brings this action to hold three U.S. persons—Marc Baier, Ryan Adams, and Daniel Gericke ("Individual Defendants")—and their former employer, DarkMatter, accountable for hacking her iPhone, surveilling her movements, and exfiltrating her confidential communications for use against her by the security services of the United Arab Emirates ("UAE").

Plaintiff's Amended Complaint addresses the issues identified by the Court in its March 13, 2023 decision, providing a factual foundation sufficient to defeat Defendants' Motion to Dismiss. First, the Amended Complaint contains allegations that Defendants committed a tort against Alhathloul in the United States by exfiltrating data from her device while they knew she was physically located here. These allegations are jurisdictionally dispositive.

Second, the Ninth Circuit, in a decision issued after this Court issued its order on the initial Motion to Dismiss, made clear that a court must assess both purposeful availment and

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

purposeful direction for jurisdiction, regardless of whether the claim sounds in tort or contract. *Davis v. Cranfield Aerospace Sols,* 71 F.4th 1154 (9th Cir. 2023). While in its prior ruling this Court applied only the purposeful direction test to assess a subset of the Amended Complaint's allegations—that Defendants targeted Apple's U.S. servers to infect Alhathloul's phone with malware—this Court must utilize both standards to evaluate the totality of the allegations in the Amended Complaint.

Third, the Amended Complaint establishes a direct connection between Defendants' hack against Alhathloul and their illegal, U.S.-based conduct described in the Individual Defendants' Deferred Prosecution Agreement ("DPA")[1] to create the Karma hacking tool and then deploy it against their targets, including Alhathloul. Among other things, the Amended Complaint alleges that Defendants recruited U.S. individuals, purchased specialized U.S. technology, and formed ongoing business relationships with U.S. companies in order to build the system used to hack Alhathloul. The Amended Complaint then describes how they deployed their attack against Alhathloul, deliberately choosing both to route their attack through Apple's U.S. servers and to utilize U.S.-based anonymization services and proxy servers they procured to elude detection. Defendants intentionally chose this hacking method, knowing that the only way it could work is by using Apple's U.S. servers. This was not accidental or fortuitous contact, but an intentional design choice. The same conduct (described in the Individual Defendants' DPA) was sufficient to support criminal jurisdiction over all three individuals in U.S. courts.

Finally, Defendants' other arguments—failure to state a claim under the Computer Fraud and Abuse Act ("CFAA") and lack of subject matter jurisdiction under the Alien Tort Statute

[1] The DPA includes the 24-page Factual Statement ("DPA Facts") attached as Exhibit A of the Amended Complaint. *See* ECF 54-1.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

("ATS")—neither of which the Court assessed in its prior ruling, still lack merit. Alhathloul's Amended Complaint states a CFAA claim anchored in facts already admitted as true by the Individual Defendants in their DPA, and further supported by the U.S. Department of State's Proposed Charging Letters for the Individual Defendants' violations of the Arms Export Control Act and International Traffic in Arms Regulations ("ITAR Facts").[2] For many of the same reasons that establish personal jurisdiction, the Court has subject matter jurisdiction over the ATS claim because it touches and concerns the territory of the United States. Significantly, the Ninth Circuit's recent decision in *Doe I v. Cisco Sys., Inc.*, 73 F.4th 700, 736, 739 (9th Cir. 2023), issued after this Court's prior ruling, confirms that an ATS claim is cognizable against Cisco for assistance allegedly provided to China even when the direct acts of surveillance occurred abroad, and directly supports this Court's exercise of jurisdiction over Alhathloul's ATS claim.

BACKGROUND

A. Defendants Developed and Operated Project Raven to Surveil Perceived Dissidents and Monitor Their Activities.

The cyber-surveillance program known as "Project Raven" originated in or about 2009, when the UAE engaged Maryland-based contractor CyberPoint International LLC ("CyberPoint"). First Amended Complaint at ECF 54 ("AC") ¶ 57. The Individual Defendants worked for CyberPoint and oversaw Project Raven's use of U.S. technology and knowhow to create the hacking tool (Karma) deployed against Alhathloul. *Id.* ¶¶ 62–64.

As CyberPoint employees, and as U.S. Persons, the Individual Defendants' activities were governed by U.S. law, including the terms of U.S. export licenses issued to CyberPoint by

[2] The Consent Agreements and Proposed Charging Letters for the Individual Defendants were attached as Exhibit B of the Amended Complaint. *See* ECF 54-2.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

the U.S. Department of State pursuant to ITAR. DPA Facts ¶ 32. The export licenses permitted CyberPoint to provide certain *defensive* cybersecurity services to the UAE, but prohibited U.S. individuals from sharing the technology with UAE companies or persons, and from engaging in *offensive* cyberattacks or targeting servers in the United States. *Id.*

To subvert these restrictions and engage in offensive hacking operations that would otherwise be prohibited, the Individual Defendants helped transition Project Raven to DarkMatter. AC ¶¶ 73–75. This transition enabled DarkMatter and the Individual Defendants to engage in widespread hacking and surveillance of perceived dissidents, including Alhathloul. AC ¶¶ 82–86, 133–39.

B. Defendants Transferred Regulated U.S. Technology and Knowhow to Target Perceived Dissidents.

Beginning around January 2016, DarkMatter took over Project Raven from CyberPoint. *Id.* ¶ 73. DarkMatter recruited U.S. individuals who held U.S. security clearances—including Defendants Baier and Adams. ITAR Facts at 5, 16. The Individual Defendants then became employees of DarkMatter. AC ¶ 75. As DarkMatter employees, the Individual Defendants operated in the same building, with the same terminals, setup, and computer infrastructure they used at CyberPoint. ITAR Facts at 5, 16. They also recruited additional U.S. persons to join the DarkMatter hacking team. AC ¶ 110.

As described in the DPA, the Individual Defendants transferred U.S. technology and knowhow—without the necessary U.S. export licenses and in violation of U.S. law—to DarkMatter. DPA Facts ¶¶ 32–33. The Individual Defendants never sought or obtained State Department licenses to continue providing services to the UAE or UAE companies, much less the offensive cyber-surveillance and hacking operations carried out as part of Project Raven. AC ¶ 177. Despite warnings from CyberPoint legal counsel, the Individual Defendants continued to

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

utilize U.S. technology and knowhow in Project Raven's hacking operations without obtaining the necessary U.S. licenses. DPA Facts ¶ 36.

C. Defendants Acquired U.S. Technology To Surveil Their Targets.

As a DarkMatter operation, run by the Individual Defendants, Project Raven actively sought more intrusive ways to surveil perceived dissidents, including by obtaining remote access to their smartphones through a highly effective hacking system known as "Karma." DPA Facts ¶¶ 44, 56.

1. Defendants Purchased Specialized Exploits and Other U.S. Technology from U.S. Companies.

In 2016, Defendants purchased specialized hacking technology—two "zero click" exploits[3]—developed and sold by companies in the United States. AC ¶¶ 93–103. These exploits were designed to leverage vulnerabilities in Apple's iMessage application, which Defendants knew used only Apple's U.S. servers. *Id.* Defendants acquired those exploits necessary to operate Karma by communicating with, entering into business relationships with, and paying more than $2,000,000 to the U.S. bank accounts of, two U.S. companies. AC ¶¶ 46, 48, 50, 52–53, 93–103. Because Defendants' acquisition of the second exploit included other computer network exploitation tools and maintenance services, Defendants established an ongoing business relationship with this U.S. company to integrate the exploit into Karma. AC ¶ 102.

2. Defendants Deliberately Interacted with U.S.-based Servers Several Times to Hack a Target.

[3] A "zero-click" exploit—such as the one used by Karma—is specialized computer code that leverages flaws in a computer's operating system to execute a command (like the installation of malware) without the device owner taking any action. DPA Facts ¶ 56.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants' design of Karma, including their particular choice of malicious code to hack its targets, was specifically intended to take advantage of vulnerabilities in Apple's Messages application, which runs iMessage. DPA Facts ¶¶ 44, 62. DarkMatter and the Individual Defendants, all sophisticated cyber-engineers, knew and understood at the time Alhathloul was hacked that the Messages application operated exclusively using servers located in the United States. AC ¶ 132. Because their chosen exploit was designed to and did rely on vulnerabilities in Apple's iMessage system, Defendants specifically intended to and did interact with Apple U.S. servers several times to deploy the hack each time they used Karma. *Id.* ¶¶ 96, 132.

- First, Defendants had to register for an Apple iMessage account and input the email address or phone number linked to the target's Apple account into Karma. *Id.* ¶ 112.
- Second, in order to send the exploit-containing iMessage, Defendants had to retrieve the target's encryption and routing information from Apple's identity servers—a group of servers located in the U.S. and on which Apple stores encryption and routing information for iMessage users. *Id.* ¶ 113.
- Third, Defendants had to send the exploit-containing iMessage, together with a payload containing malware, to Apple's iMessage servers in the U.S. to reach their target's iPhone. *Id.* ¶ 114.

As Project Raven's experts in computer network exploitation, Defendants Baier, Adams, and Gericke each possessed a technical understanding of how the Karma exploits functioned, including that the exploits relied on Apple's U.S. servers to reach a target's device. *Id.* ¶ 132.

3. Defendants Eluded Detection by Using U.S.-based Anonymization Services and Proxy Servers.

Defendants enhanced Karma with additional technology, including computer hardware located, built, or purchased in the United States. *Id.* ¶¶ 87–110. Because the exploits did not

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

have an anonymous delivery mechanism, Defendants utilized a U.S. company's anonymization services and proxy servers to mask the origin of their hacking transmissions, which otherwise could have been traced back to DarkMatter by Apple. DPA Facts ¶¶ 39, 47, 49, 54, 56. By routing their network activity through these U.S.-based anonymization services and proxy servers, Defendants evaded detection and attribution of their attacks, allowing Defendants to persist with the hacking. AC ¶¶ 107–109. These enhancements helped make Karma effective in 90 to 95% of deployments. *Id.* ¶ 109.

4. Defendants Used Apple's U.S.-Based Servers to Install Malware on a Target's Device to Exfiltrate Data.

Defendants used Apple's U.S. servers to send the exploit to a target's device, causing the device to run the exploit code without the target's awareness or authorization. AC ¶¶ 87–89. Upon execution, the exploit code installed malware[4] on the target's iPhone; the malware then could view, access, and modify data within the Messages app, and, ultimately, all data on the iPhone. *Id.* ¶¶ 123–24. The final step of the attack occurred when the installed malware connected to a server controlled by Project Raven to exfiltrate data from the device. *Id.* ¶ 126. Devices that were compromised by Karma *continuously* transmitted data stored on the compromised device to servers controlled by Project Raven. *Id.* ¶ 127.

D. Defendants Hacked and Surveilled Alhathloul.

Project Raven hacked Alhathloul's iPhone in 2017 using Karma. AC ¶¶ 134–36. During the course of their surveillance of Alhathloul, Defendants assigned her the codename "Purple Sword." *Id.* Defendants met regularly with the UAE's National Electronic Security Authority to receive designated targets and share intelligence collected on those targets. *Id.* ¶ 67. Defendants

[4] Malware is code that is unwanted by the device owner; it may perform various functions, including allowing access to, collection, deletion, or modification of data on the device. AC ¶ 89.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

used Karma to hack into the iPhones of hundreds of perceived dissidents, and each of the Individual Defendants admitted in their DPA that they used Karma to "gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers…*including on computers and servers in the United States*, as well as computers and servers that communicated with computers in the United States," in violation of U.S. law. DPA Facts ¶ 1 (emphasis added).

Project Raven's cyber-surveillance often focused on a perceived dissident's communications with individuals and organizations located globally. For instance, in 2016, Project Raven hacked a perceived dissident—Ahmed Mansoor—for his ongoing efforts to draw attention to human rights violations across the Middle East and intercepted communications between Mr. Mansoor and international non-governmental organizations ("NGOs"). AC ¶¶ 46, 83. In 2017, Mr. Mansoor was charged, convicted and sentenced to ten years in prison, based, in part, on hacked email exchanges and encrypted WhatsApp messages between himself and representatives of Human Rights Watch, Amnesty International, and the Gulf Centre for Human Rights. *Id*. ¶ 46.

Project Raven targeted Alhathloul in 2017 by sending the exploit to Alhathloul's device and causing the exploit code to install malware on Alhathloul's iPhone. AC ¶¶ 134–39. This malware provided Defendants with constant and continuous access to location data and data from applications on Alhathloul's device—such as iMessages, email, Facebook, WhatsApp, and Telegram—and allowed DarkMatter to continuously monitor Alhathloul's whereabouts and surveil her private communications. *Id.*

1. Defendants Surveilled Alhathloul To Monitor Her Communications with U.S. Journalists and Non-Governmental Organizations.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

As an advocate on behalf of women and girls in Saudi Arabia, Alhathloul gained widespread recognition in the United States, with U.S. news organizations regularly reporting on her work. AC ¶¶ 16–18.

Alhathloul regularly communicated with journalists and NGOs in the United States to build international support for reforms in Saudi Arabia. *Id.* ¶ 24. In October 2016, Alhathloul participated in a documentary produced by *The New York Times* and targeted to a largely U.S.-based audience; Alhathloul told the story of her arrest in 2014, when she attempted to drive from the UAE to Saudi Arabia. *Id.* ¶ 25. Throughout 2016, Alhathloul collaborated with Human Rights Watch, an NGO headquartered in New York, to contribute research to its report *Boxed In: Women and Saudi Arabia's Male Guardianship System*, which called for the end of male guardianship in Saudi Arabia. *Id.* ¶ 26. Alhathloul frequently corresponded with Human Rights Watch researchers in the United States. *Id.* Alhathloul regularly communicated with other human rights advocates living in the United States and often traveled internationally advocating for women's rights in Saudi Arabia. *Id.* ¶¶ 28–30.

Because Alhathloul suspected that her activities were being closely monitored by the Saudi government, she took precautions when communicating with journalists, advocates, and NGOs. *Id.* ¶ 152. Alhathloul specifically chose to use her iPhone because of its reputation for enhanced security features and her knowledge that it relied on servers located in the United States. *Id.* Like her community of human rights advocates, Alhathloul generally trusted the safety of iPhones and chose to use, for example, iPhone's FaceTime application, believing it offered one of the few modalities for secure video communication. *Id.* The object of the hack was to allow DarkMatter to surveil Alhathloul's iPhone communications with other human rights

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

advocates, researchers, and journalists, including U.S.-based human rights advocates, researchers, and journalists. *Id.* ¶ 140–42, 149.

2. Defendants Surveilled Alhathloul While She was Physically Present in the United States.

In November 2017, Alhathloul was invited to Washington, D.C as an honored speaker at an event hosted by the Arab Gulf States Institute—"Driving Forward: Women in the Gulf Assess a Changing Landscape." *Id.* ¶ 143. Alhathloul's trip to the United States was pre-planned and widely publicized on social media. *Id.* ¶¶ 144–46. Alhathloul traveled to the United States to attend the event and discuss her advocacy work before an audience of largely U.S. individuals. *Id.* ¶¶ 143–47.

Alhathloul brought and used her iPhone—the iPhone that unknown to her had been hacked and was being used to regularly exfiltrate her data—during her visit. *Id.* ¶ 148. From November 28, 2017 until her return to the UAE on December 2, 2017, Alhathloul used the device to communicate with friends, family, and other human rights advocates, including individuals living in the United States. *Id.* Alhathloul was unaware that her iPhone was corrupted at the time. *Id.* ¶ 155.

Not only was Alhathloul's U.S. trip widely publicized, Defendants continuously surveilled Alhathloul's communications and the location data of her iPhone and therefore would have known that Alhathloul was in the U.S. and using her device there. *Id.* ¶¶ 142, 150. During their continuous surveillance of Alhathloul's communications and whereabouts, Defendants exfiltrated private encrypted data from her device while she was physically present in the United States. *Id.* ¶ 150. The data exfiltrated by Defendants included her confidential communications with U.S.-based human rights advocates, researchers, and journalists, as well as messages she sent while physically present in the United States. *Id.* ¶ 149.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

3. Defendants' Hack Led to Alhathloul's Arrest and Rendition to Saudi Arabia Where She Was Detained, Tortured, and Prosecuted.

Defendants' hack allowed the UAE security services to track Alhathloul's whereabouts and monitor her activities. *Id.* ¶ 142. As a result, on March 13, 2018, shortly after her trip to the United States, the UAE security services arrested and arbitrarily detained Alhathloul, then rendered her to Saudi Arabia where she subsequently suffered abuses at the hands of the Saudi government. *Id.* ¶¶ 156–57.

Saudi authorities placed her on a travel ban, raided her family home in Riyadh, arrested her and transferred to her to multiple prisons. *Id.* ¶¶ 160–63. At a secret prison in Jeddah, Saudi authorities interrogated Alhathloul and tortured her, including subjecting her to electric shocks and beatings. *Id.* ¶ 164. During her interrogation and torture, her interrogators confronted her with details about her private communications that could only be obtained through unlawful access of her electronic device. *Id.* ¶ 165. Following her arrest, Saudi Arabia held Alhathloul without charges or trial for ten months. Her arrest and detention disrupted Alhathloul's ongoing work with U.S.-based human rights advocates, researchers, and journalists. AC ¶ 154.

Alhathloul was ultimately tried by the Specialized Court of Saudi Arabia. *Id.* ¶ 167. The Saudi charging documents referenced private communications stored on her iPhone, including private communications that had been transmitted via Telegram and WhatsApp, both end-to-end encrypted messaging services. *Id.* ¶ 169. The charging document also referenced Alhathloul's participation in conferences and panels relating to Saudi women's rights, her contacts with international organizations and foreign journalists, and her communications with human rights advocates and NGOs located abroad, including in the United States. *Id.* ¶ 170.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Should Defendants contend that there is insufficient detail pled to support these or any other factual allegations or reasonable inferences, particularly regarding matters within the exclusive control of Defendants, Alhathloul reserves the right to seek jurisdictional discovery.

STANDARD OF REVIEW

To defeat a Rule 12(b)(2) dismissal for lack of personal jurisdiction, the plaintiff need only identify "facts that if true would support jurisdiction." *Ballard v. Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995). In considering a motion to dismiss under Rule 12(b)(6), the Court must "accept [Plaintiff's] allegations as true and construe them in the light most favorable to plaintiff[]." *Curry v. Yelp Inc.*, 875 F.3d 1219, 1224 (9th Cir. 2017). The same standard applies for Defendants' arguments under Rule 12(b)(1), as Defendants present a facial, not factual attack, and "argue that the allegations in [the] complaint are insufficient on their face to establish subject matter jurisdiction." *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004).

ARGUMENT

I. DEFENDANTS HAVE SUFFICIENT MINIMUM CONTACTS WITH THE UNITED STATES.

Defendants do not contest that, (a) because Alhathloul asserts claims under federal law, and (b) Defendants have maintained they are not subject to general jurisdiction anywhere in the United States, the relevant jurisdictional question is whether Defendants have sufficient "minimum contacts" *with the United States as a whole* such that "the maintenance of the suit does not offend traditional notions of fair play and substantial justice." *Freestream Aircraft (Berm.) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 602 (9th Cir. 2018); *see* Fed. R. Civ. P. 4(k)(2). Defendants also do not contest that the evaluation must consider all contacts with the United States, and is not limited to contacts with any specific state. ECF 63 at 13, 26.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

The minimum contacts test requires that (1) a defendant either perform some act by which they purposefully avail themselves of the forum, or alternatively, purposefully direct their activities at the forum; (2) the plaintiff's claim "arise out of or relate[] to" this conduct; and (3) the exercise of jurisdiction be reasonable. *Freestream*, 905 F.3d at 603.

Defendants argue that only the purposeful direction test, and not purposeful availment, is relevant to the Court's analysis. But that is contrary to the Ninth Circuit's recent decision in *Davis*, which clarified that there is no "rigid dividing line" that dictates applying purposeful availment to contract claims and purposeful direction to tort claims. *Davis*, 71 F.4th 1154, 1162 (9th Cir. 2023) (quoting *Glob. Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.*, 972 F.3d 1101, 1107 (9th Cir. 2020)). Instead, when assessing minimum contacts courts must "comprehensively evaluate the extent of the defendant's contacts with the forum state and those contacts' relationship to the plaintiffs' claims—which may mean looking at both purposeful availment and purposeful direction," to ask "whether defendants have voluntarily derived some benefit from their interstate activities such that they 'will not be haled into a jurisdiction solely as a result of 'random,' 'fortuitous,' or 'attenuated' contacts.'" *Id.*

Defendants' extensive contacts with the United States to develop and deploy Karma against Alhathloul satisfy both purposeful availment and purposeful direction. Significantly, the Amended Complaint alleges that DarkMatter exfiltrated data from Alhathloul's iPhone while she was physically present in the United States and thereby committed tortious conduct—accessing data on a protected computer without authorization—in the forum. *See* 18 U.S.C. § 1030(a)(2)(C). Although Defendants profess their lack of intent to hack Alhathloul *here*, that carries no weight at the motion to dismiss stage, especially so when the Amended Complaint plausibly alleges that their tortious conduct in the forum was knowing and deliberate.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

While this conduct alone establishes a jurisdictionally adequate connection between Defendants and the forum, Defendants' numerous other forum contacts, occurring at nearly every step of Defendants' hack, also support the exercise of jurisdiction. Among other things, Defendants recruited U.S. cyber-security experts, purchased specialized U.S. technology, and formed ongoing business relationships with U.S. companies in order to build the system used to hack Alhathloul. Defendants then deployed their hack against Alhathloul by deliberately transmitting malicious code to Apple's U.S.-based servers and utilizing U.S.-based anonymization services and proxy servers to facilitate the hack and elude detection.

A. Defendants Purposefully Availed Themselves of U.S. Jurisdiction by Committing Tortious Hacking Activity in the United States.

Defendants' exfiltration of data from Alhathloul's iPhone located in the United States is dispositive of jurisdiction because of the "well-settled understanding that the commission of a tort within the forum state usually supports the exercise of personal jurisdiction." *Freestream*, 905 F.3d at 606 (applying the purposeful availment test from *Paccar Int'l, Inc. v. Commercial Bank of Kuwait, S.A.K.*, 757 F.2d 1058 (9th Cir. 1985)). The Amended Complaint alleges that Defendants continuously surveilled Alhathloul, tracked her whereabouts and communications (such that they knew she and her device were in the United States), and exfiltrated data from her device while it was located in the United States. By exfiltrating data from Alhathloul's device while it was located here, Defendants committed tortious actions in the forum.[5] *See* 18 U.S.C. § 1030(a)(2)(C) (prohibiting the intentional access, without authorization, of a protected computer to obtain information).

[5] Although Defendants also committed CFAA violations "by causing the transmission" of exploitive code, in violation of 18 U.S.C. § 1030(a)(5)(A), the exfiltration of data from her device is a separate tortious act under the CFAA.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants would have the Court ignore this by characterizing their conduct as due to the mere chance of Alhathloul's "voluntarily travel[]." ECF 63 at 16. But the voluntariness of her travel to the U.S. is not jurisdictionally relevant; she was here, and jurisdiction exists when a defendant commits a tort in the forum. *See Freestream*, 905 F.3d at 603 (9th Cir. 2018) (citing on *Paccar*, 757 F.2d at 1064).

Defendants' reliance on *Walden v. Fiore*, 571 U.S. 277 (2014) is inapposite. *Walden* held that jurisdiction cannot be established merely by virtue of the plaintiff's residence, without the defendant committing some other acts in the forum. This is not Alhathloul's asserted basis for jurisdiction. Here, jurisdiction is based on Defendants' knowing exfiltration of data from Alhathloul's device *in the forum—Walden* did not upset long-standing precedent that the commission of an intentional tort in the forum establishes jurisdiction. That is why this Court reasoned that a defendant availed itself of the forum, "and not just with persons who reside [there]," when the defendant "knew that [a] server was located [in the forum] and then themselves retrieved items from that server for an unauthorized purpose." *Climax Portble Mach. Tools, Inc. v. Trawema GmbH*, No. 3:18-cv-1825-AC, 2020 U.S. Dist. LEXIS 47790, at *18 (D. Or. Mar. 19, 2020) (applying *Walden*). The Amended Complaint alleges that, through their active surveillance of Alhathloul's communications and whereabouts, Defendants knew of her presence in the United States and nonetheless continued their unlawful access to her device and exfiltrated data from the device while she was here. Indeed, Defendants' exfiltration of data from Alhathloul's device in the United States was similar to the numerous other occasions Defendants "acquire[d] data from computers, electronic devices, and servers...in the United States," which supported U.S. criminal jurisdiction. DPA Facts ¶ 1.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

While the exfiltration of data from Alhathloul's device in the forum establishes a "single sufficiently deliberate contact" to satisfy purposeful availment, Defendants' numerous other forum contacts reinforce this Court's exercise of jurisdiction. *Yamashita v. LG Chem, Ltd.*, 62 F.4th 496, 504 (9th Cir. 2023). Defendants also purposefully availed themselves of the forum by using U.S. servers at multiple points in their attack against Alhathloul. Acting through the internet, Defendants *virtually* entered the United States to access Alhathloul's iMessage credentials on Apple's U.S. servers and then deliberately sent its exploit and malware to Apple's U.S. iMessage servers to cause these servers to transmit malware to Alhathloul's iPhone. While many courts have found that knowing and purposeful access of servers in the forum is sufficient to find purposeful availment, *see* ECF 35 at 25, the Amended Complaint also alleges that Defendants acquired and used other U.S.-based technology—a U.S. company's anonymization services and proxy servers—in the hack against Alhathloul. Because Defendants "specifically chose" these U.S.-based anonymization services and proxy servers to mask the origin of its transmissions from the UAE, their conduct satisfies purposeful availment. *See 42 Ventures, LLC v. Mav*, No. 20-00228 DKW-WRP, 2022 U.S. Dist. LEXIS 117109, at *12 (D. Haw. June 15, 2022), *report and recommendation adopted*, CV 20-00228 DKW-WRP, 2022 WL 2392484, at *4 (D. Haw. July 1, 2022) (finding purposeful availment when foreign defendant "specifically chose" servers in the United States "to overcome blacklist restrictions").

Finally, Defendants' abundant other forum contacts—at nearly every stage of its creation and operation of Project Raven—supports jurisdiction because purposeful availment looks at "a defendant's 'entire course of dealing' with the forum" and "not solely the particular contract or tortious conduct giving rise to [a claim]." *Davis*, 71 F.4th at 1163 (quoting 972 F.3d at 1108). DarkMatter recruited individuals with U.S. security clearances, such as the

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Individual Defendants, to work on Project Raven, illegally transferred technology—otherwise protected by U.S. export licenses—and assembled it into a tool used to hack Alhathloul and other perceived dissidents.

Defendants purchased specialized exploits, developed in the United States, and sold by two U.S. companies, to create the specific tool (Karma) used to hack and surveil Alhathloul. Defendants paid by transferring funds into the U.S. bank accounts of these two U.S. companies. *Licci v. Lebanese Canadian Bank*, 732 F.3d 161, 171 (2d Cir. 2013) ("[S]election and repeated use of New York's banking system, as an instrument for accomplishing the alleged wrongs for which the plaintiffs seek redress" shows purposeful availment). Defendants entered into contracts with these U.S. companies to purchase the exploits, and formed an ongoing business relationship with at least one, in order to effectively use the exploit. *Davis*, 71 F.4th at 1163 ("Purposeful availment can be established by a contract's negotiations, its terms, its contemplated future consequences, and the parties' actual course of dealing") (citing *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 479 (1985)).

Defendants did all of this so that they could "take advantage of vulnerabilities in common software and operating systems created by [Apple]," DPA Facts ¶¶ 44, 62, and infiltrate the iPhone of Alhathloul and the iPhones of other perceived dissidents like her. Alhathloul, like her community of women's rights and human rights advocates, specifically chose to use an iPhone because of its reputation for enhanced security features and knowledge that it relied on servers located in the United States. *Yamashita*, 62 F.4th at 503 (purposeful availment involves assessing whether the defendant "deliberately reached out beyond [its] home—by, for example, exploiting a market in the forum State").

B. Defendants Purposefully Directed Their Tortious Actions at the United States.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants purposefully directed their tortious actions at the United States. To assess purposeful direction, courts apply a three-part "effects test," which requires that the defendant commit an intentional act that is expressly aimed at the forum and causes harm that the defendant knows is likely to be suffered in the forum. *Calder v. Jones*, 465 U.S. 783, 790-91 (1984).

1. Defendants Expressly Aimed Their Conduct at the United States.

First, Defendants' exfiltration of data from Alhathloul's device, a protected computer, while it was located in the United States, satisfies express aiming. The Ninth Circuit, this Court, and numerous others have held that express aiming occurs when a defendant accesses a plaintiff's protected computer in the forum to commit a tort. *See, e.g.*, *DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018) (defendant used forum-located server to commit copyright infringement); *Climax*, 2020 U.S. Dist. LEXIS 47790 at *20-21; *MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012); *Felland v. Clifton*, 682 F.3d 665, 676 n.3 (7th Cir. 2012) (defendant sent fraudulent emails through forum-located server); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 826 (N.D. Cal. 2014) (foreign defendant took confidential information from server that he had reason to know was in forum) (collecting similar cases).

Again, Defendants' reliance on *Walden* is misplaced. Although Defendants did not control Alhathloul's travel to the United States, they did control their own actions taken after they knew she traveled to the United States. *DEX*, 727 F. App'x at 278 (explaining that "[w]here *Walden* featured an alleged tort committed against a forum resident outside the forum state," here the tort occurred on plaintiff's server "in the forum state"); *Oregon Int'l Airfreight Co. v. Bassano*, No. 3:21-cv-01480-SB, 2022 U.S. Dist. LEXIS 102322, at *12 (D. Ore. May 16, 2022) (finding allegation that defendant knew of server's location satisfied express aiming).

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Second, although this Court previously found that "[m]ere knowledge of the location of a third-party's servers...is not sufficient to constitute purposeful direction," the Amended Complaint now makes clear that Defendants expressly aimed their tortious conduct at the forum by utilizing U.S.-based anonymization services and proxy servers and Apple's U.S.-based servers to hack Alhathloul's iPhone. Defendants' deliberate choice to use U.S.-based anonymization services and proxy servers "establishes a meaningful connection between its conduct and the forum." ECF 44 at 13; *see also Will Co., Ltd. v. Lee*, 47 F.4th 917, 924 (9th Cir. 2022) (finding foreign defendants' use of an in-forum server was not fortuitous where "Defendants chose to host the website in Utah. . . ."). By using U.S.-based anonymization services and proxy servers to mask the origin of their malicious transmissions, Defendants' conduct falls squarely within the type that satisfies express aiming. *AMA Multimedia, Ltd. Liab. Co. v. Wanat*, 970 F.3d 1201, 1212 n.8 (9th Cir. 2020) (identifying "reli[ance] on U.S.-based servers"); *HB Prods., Inc. v. Faizan*, 603 F. Supp. 3d 910, 932 (D. Haw. 2022) ("Defendant sought a United States-based IP address to circumvent blacklist restrictions"); *42 Ventures*, 2022 U.S. Dist. LEXIS 117109, at *12 ("specifically chose" U.S. servers "to overcome blacklist restrictions").

The Amended Complaint also shows how Defendants' transmission mechanism for the exploit utilized Apple's U.S. servers. This was no accident; it was deliberate and by design. Defendants' professional expertise and involvement in the creation of Karma leave no doubt that they deliberately chose to utilize an exploit that relied upon Apple's U.S. servers—rather than numerous other methods to insert malware onto Alhathloul's iPhone—because it rendered the malicious transmission undetectable to even a sophisticated user like Alhathloul. This secretive

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

transmission mechanism, which could only occur through Apple's U.S. servers, was central to Defendants' surveillance.

The principal authority upon which Defendants rely, *Hungerstation*, held that jurisdiction over a foreign entity is not proper "solely because" the out-of-forum defendant simply logged into a computer terminal and remotely accessed a server that could have been anywhere (but was fortuitously located in the United States). *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349, 351 (9th Cir. 2021); *Will Co.*, 47 F.4th at 926 (distinguishing *Hungerstation* and similar cases because that authority "simply states that the location of the server alone is insufficient to establish personal jurisdiction, *not that it is irrelevant to the analysis*") (emphasis added). By contrast, Alhathloul specifically chose to use an iPhone because of its security and knowledge that it relied on servers located in the United States. In turn, Defendants specifically chose to hack her otherwise secure iPhone by using a zero-click exploit that by design utilized Apple's U.S. servers. Nothing about this U.S.-based conduct was fortuitous.

Third, Defendants' surveillance sought (and in fact did collect) communications between Alhathloul and U.S. journalists, NGOs, and human rights advocates, and thus "had 'a [U.S.] focus' because [it] concerned 'the plaintiff's activities in [the United States].'" *Burri Law Pa. v. Skurla*, 35 F.4th 1207, 1214 (9th Cir. 2022) (applying *Walden* and *Calder*). Like other perceived dissidents, Project Raven sought to surveil Alhathloul's activities domestically and abroad, which for Alhathloul included her communications with U.S. individuals. The ongoing exfiltration of Alhathloul's communications, together with the fact that these communications were mentioned in her Saudi charging documents, belies the notion that her U.S. communications were incidental to Defendants' hacking activity. *See also S.D. v. Hytto Ltd.*, No. 18-cv-00688-JSW, 2019 U.S. Dist. LEXIS 229909, at *11 (N.D. Cal. May 14, 2019)

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

(finding express aiming when foreign company "intercept[ed]" user-to-user communications and "knew" that "some" users were residents of the U.S.). The fact that Defendants directed the exploit itself to Alhathloul's iPhone does not undercut Defendants' express aiming at the United States because a substantial part of Project Raven's surveillance involved her U.S. communications. *Dudnikov v. Chalk & Vermilion Fine Arts, Inc.*, 514 F.3d 1063, 1075 (10th Cir. 2008) (Gorsuch, J.) (analogizing conduct expressly aimed at the forum to a "bank shot in basketball" when the defendant sent an email to California with the express aim to interfere with plaintiff's event in Colorado).

2. Defendants Caused Harm That They Knew Was Likely to be Suffered in the Forum.

Defendants' tortious conduct caused harm that they knew was likely to be suffered in the United States. Under the effects test, the plaintiff need not suffer the "brunt of the harm" in the forum, only a "jurisdictionally sufficient amount of harm." *Yahoo! Inc. v. La Ligue Contre Le Racisme*, 433 F.3d 1199, 1207 (9th Cir. 2006). Courts assess whether a defendant has caused harm in the forum by looking at whether the "'bad acts' that form the basis of the plaintiff's complaint occur in that forum." *Will Co.*, 47 F.4th at 926 (citation omitted). Here, the exfiltration of a data from Alhathloul's device while she was in the United States clearly comprises a "bad act" and jurisdictionally significant harm because the exfiltration of data from her device—a prohibited act under the CFAA—occurred in the United States. *See* 18 U.S.C. § 1030(a)(2)(C). The allegations that Defendants constantly monitored Alhathloul's communications and whereabouts show that they *knew* her device was in the United States and thus the harm would be suffered here. Defendants attempt to draw a distinction between where this exfiltration occurred (at least, in part, in the United States) and where Alhathloul was when she "discover[ed]" she had been surveilled. ECF 63 at 19. But Defendants cite no authority to

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

support its novel argument that harm is "felt" only where a plaintiff is physically situated when they *subsequently learn* the tort occurred, rather than where the tort actually occurred.

Defendants' tortious surveillance of Alhathloul's communications with U.S. journalists, NGOs, and advocates independently satisfies the requirement that they knew she would suffer harm in the United States. Regardless of where her device was located when Defendants accessed her confidential communications, because her communications were both sent to and received from the United States, a jurisdictionally significant amount of harm occurred in the United States when Defendants improperly accessed those communications.

C. Defendants' Contacts with the United States Relate to Alhathloul's Claims.

Alhathloul's claims "arise out of or relate to [Defendant's] contacts with the forum," such that there is "an affiliation between the forum and the underlying controversy." *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 141 S. Ct. 1017, 1028 (2021) (citations omitted).

"The first half of that standard asks about causation," which Alhathloul satisfies, because her claims are based on Defendants' exfiltration of data from her device—their tortious conduct—in the forum. *Id.*; *Freestream*, 905 F.3d at 603 ('"The commission of an intentional tort in a state is a purposeful act that will satisfy the first two requirements of the minimum contacts test."') (citing *Paccar*, 757 F.2d at 1064).

The standard's "back half, after the 'or,' contemplates that some relationships will support jurisdiction without a causal showing," and is independently satisfied by Defendants' other extensive U.S. contacts to carry out Project Raven, create of Karma, and hack Alhathloul. *Ford*, 141 S. Ct. 1017 at 1026. Defendants ignore the essential connection between, among other things, their acquisition of technology from the United States and their surveillance of Alhathloul.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

In the Ninth Circuit's recent *Yamashita* decision, the court applied *Ford* and identified three "guid[ing]" factors to determine whether the defendant's forum contacts were "sufficiently related to the plaintiff's injury"— (1) if "similar injuries will tend to be caused by those contacts," that is, even if causation cannot be proven, the conduct was likely to injure someone similarly situated; (2) "if the defendant should have foreseen the risk that its contacts might cause injuries like that of the plaintiff"; or (3) there was a "a close connection between contacts and injury." *Yamashita*, 62 F.4th at 505-06. Alhathloul meets all three factors.

First, Defendants admitted that they used Karma and Apple's U.S. servers "to gain unauthorized access to the corresponding accounts, systems, and servers, *some of which were located in the United States*." DPA Facts ¶ 59 (emphasis added). Alhathloul's iPhone was located in the United States and Defendants are alleged to have known it and exfiltrated data anyway. Thus, Alhathloul's specific claims relate to Defendants' in-forum conduct.

Second, not only should Defendants "have foreseen the risk that [their] contacts might cause injuries like that of the plaintiff," the entire point of Defendants' acquisition of U.S. exploits, transferring export-controlled U.S.-technology, and leveraging Apple's U.S.-based servers, was to target individuals such as Alhathloul. *Yamashita*, 62 F.4th at 505–06. Defendants claim that they "altered" the U.S.-purchased exploits before using them has no bearing on relatedness. ECF 63 at 22. Defendants enhanced the exploits because they "did not have an anonymous delivery mechanism," DPA Facts ¶¶ 47, 54, and these enhancements also involved their U.S. contacts. *See* AC ¶ 105.

Third, there is a close connection between Alhathloul's claims and Defendants' forum contacts. Every U.S. contact alleged relates to Defendants' development and installation of the very exploit used to exfiltrate data from Alhathloul device while she was in the United States and

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

elsewhere. The same conduct underlying Alhathloul's claims—the deliberate transmission of exploits to Apple's U.S servers to hack the iPhones of Project Raven's targets—resulted in Defendants' access to protected computers, Alhathloul's among them, in the United States.

D. Defendants Fail to Show Jurisdiction is Unreasonable.

Once a plaintiff establishes that the first two prongs of the minimum contacts test are met, the burden shifts to the defendant to demonstrate the exercise of jurisdiction would be unreasonable. *Burger King*, 471 U.S. at 476–78. Defendants fail to meet that burden, and raise only mere inconveniences and speculative concerns, under the Ninth Circuit's seven-factor balancing test. *Freestream*, 905 F.3d at 607

First, Defendants repeatedly and purposefully interjected themselves into the United States' affairs by exfiltrating data from a protected computer located in the United States, exploiting vulnerabilities in Apple's (a U.S. company) iMessage system, deliberately transmitting exploitive code into the United States, and using U.S. servers and technology. While Defendants' hack targeted Alhathloul, a nonresident, they sought information about her communications with U.S. individuals and her affairs in the forum. *See Ghuman v. Nicholson*, No. CV-20-02474-PHX-DLR, 2021 U.S. Dist. LEXIS 32674, at *7 (D. Ariz. Feb. 22, 2021) (finding purposeful interjection when the defendant's conduct involved "repeatedly communicating with individuals that he knew or should have known were [forum] residents in an effort to interfere with the [plaintiff's] personal and economic affairs in [the forum]").

Second, Defendants raise only a minimal burden of defending in this suit in the United States. The Individual Defendants are currently involved in other legal proceedings in the United States and are represented by U.S. counsel, admitted the existence of U.S. jurisdiction when they entered into the DPA, and the DPA imposes continual obligations on the Individual Defendants for the term of the agreement. DPA ¶ 9 (requiring annual disclosures). DarkMatter

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

has U.S. counsel for this case and recently defended another case in U.S. courts. ECF 35 at 34. *See In re Zf-Trw Airbag Control Units Prods. Liab. Litig.*, No. LA ML19-02905 JAK (FFMx), 2022 U.S. Dist. LEXIS 32593, *51 (C.D. Cal. Feb. 9, 2022) (finding familiarity with the United States legal system and retention of U.S. counsel are mitigating factors in assessing reasonableness). Notably, DarkMatter has also marketed its services to companies in the United States and routinely sent employees to the U.S. for this purpose. AC ¶ 7. *Hurt v. Commerce Energy, Inc.*, No. 1:12-CV-00758, 2013 U.S. Dist. LEXIS 122641, at *14 (N.D. Ohio Aug. 27, 2013) (finding lessened burden when defendant markets in the forum and its employees travel there).

This minimal burden must be weighed against the burden on Alhathloul to litigate in the UAE. *Sinatra v. Nat'l Enquirer, Inc.*, 854 F.2d 1191, 1199 (9th Cir. 1988). There is little doubt that Alhathloul, who is still unable to leave Saudi Arabia because of a travel ban, would be unable to receive a fair trial in the UAE, and would likely face threats to her personal safety if she even attempted to bring her claims there.

Third, Defendants merely assert, without further explanation, that an "obvious conflict exists between jurisdiction here and the sovereignty of the UAE and Saudi Arabia…." ECF 44 at 21. Defendants' argument proves too much: it would mean no private company working for a foreign government could be liable for its conduct. *See Cisco,* 73 F.4th at 737. Regardless, Alhathloul's claims "seek[] only the determination and enforcement" of U.S. laws against the individuals and private corporation involved, not those governments. *Ayla, LLC v. Alya Skin Pty. Ltd.*, 11 F.4th 972, 984 (9th Cir. 2021).

While courts must consider the "procedural and substantive interests of other nations" in deciding whether to exercise jurisdiction, this inquiry commonly focuses on the foreign state's

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

"particular interest in adjudicating th[e] suit." *Asahi Metal Indus. Co. v. Superior Court of Cal.*, 107 S. Ct. 1026, 1034 (1987); *Harris Rutsky & Co. Ins. Servs. v. Bell & Clements Ltd.*, 328 F.3d 1122, 1133 (9th Cir. 2003) (identifying adjudicatory interest of sovereign). Defendants fail to identify any such legitimate interest either the UAE or Saudi Arabia may have in adjudicating the violations of U.S. law alleged here. There is no cognizable "clash" because (a) crimes against humanity, subject of the ATS claims, are part of customary international law (and therefore binding on all states); and, (b) the U.S.'s interest in protecting against the abuse of U.S. computer systems that underlie the CFAA exists regardless of the other countries' interests. *See Asahi Metal*, 480 U.S. at 115. The only interest that Defendants seem to hint at—the UAE's policy of surveilling perceived dissidents—cannot shield Defendants from answering for violations of U.S. law, as demonstrated by the Individual Defendant's criminal prosecution covered by the DPA.

Fourth, the United States' interest in adjudicating this civil case is compelling. The DPA itself demonstrates that the United States has an interest in regulating the violations of U.S. law and the harm that occurred in this case, and even anticipates the possibility of civil suits arising out of this conduct. DPA ¶ 24 ("This Agreement does not provide any protection for any other criminal or civil matter."). Both the ATS and CFAA reflect the interest of the United States in broadly protecting against crimes against humanity and intrusions on U.S. computer systems, respectively.[6]

Fifth, because Alhathloul's claims "rest on the law of … the United States," and involves tortious conduct that occurred here, the United States provides "the most efficient judicial

[6] A bipartisan group of U.S. legislators recently introduced a bill to prohibit assistance to foreign governments that use spyware to violate human rights. *See* Protecting Americans from Foreign Commercial Spyware Act, H.R. 5440, 118th Cong. § 1 (2023).

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

resolution of the controversy." *Ayla*, 11 F.4th at 984. Although some "relevant parties, documents, and witnesses" likely are located abroad, many others likely are located in the United States—for example, Apple's technology experts and the companies that designed and sold the exploits used by Defendants. In any event, this factor is no longer weighed heavily. *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1323 (9th Cir. 1998).

Sixth, this forum is most likely to provide "convenient [and] effective relief" because Alhathloul's claims arise under U.S. law. *Id.* at 1324. Indeed, U.S. courts are likely *the only* available venue for any relief, especially under the ATS and CFAA. She cannot realistically be expected to bring claims in the courts of the very countries that denied her human rights, as neither would provide an effective venue. And although the Ninth Circuit may have "given little weight to the plaintiff's inconvenience" in this factor, *Panavision*, 141 F.3d at 1324, it has not forsaken "effectiveness."

Seventh, the burden of demonstrating the lack of an alternative forum "becomes an issue only when the forum state is shown to be unreasonable." *Sinatra*, 854 F.2d at 1201. In any event, the Amended Complaint's allegations show that the UAE is not a viable alternative forum.

II. THE COMPLAINT VALIDLY ALLEGES VIOLATIONS OF THE CFAA

There is no merit to Defendants' argument that Alhathloul fails to state a claim under the CFAA. To do so, she must allege that (1) Defendants intentionally accessed, or transmitted a program, information, code, or command to; (2) Alhathloul's protected computer; (3) thereby causing damage to the device; and (4) Alhathloul suffered loss greater than $5,000 or physical injury. See 18 U.S.C. § 1030(g); 18 U.S.C. § 1030(c)(4)(A)(1) (listing predicate harms for civil claim).

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

A. Alhathloul's Hacked Phone Qualifies as a "Protected Computer."

Congress expressly authorized the CFAA's extraterritorial application. *See In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 4498 (N.D. Cal. 2018) (citing *U.S. v. Ivanov*, 175 F. Supp. 2d 367, 375 (D. Conn, 2001) (holding Congress "has clearly manifested its intention" to apply the CFAA extraterritorially)). The CFAA's scheme of prohibited actions concerns "protected computer[s]." 18 U.S.C. § 1030(a)(1). Under the statute, a "protected computer":

> means a computer— (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States . . .

18 U.S.C. § 1030(e)(2). "An internet connection is sufficient for a computer to be 'used in interstate or foreign commerce." *Prop. Rights Law Grp., P.C. v. Lynch*, No. 13-00273 SOM/RLP, 2014 U.S. Dist. LEXIS 74259, at *39 (D. Haw. May 30, 2014) (citing *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) ("With a connection to the Internet, the Salvation Army's computers were part of "a system that is inexorably intertwined with interstate commerce" and thus properly within the realm of Congress's Commerce Clause power.")); *see also Mifflinburg Tel., Inc. v. Criswell*, 277 F. Supp. 3d 750, 791 (M.D. Pa. 2017) (noting that the definition of "protected computer" "embraces any computing device that may be used in interstate commerce").

Alhathloul has pled allegations sufficient to meet these requirements—specifically, that her hacked device was an iPhone, and that that iPhone was connected to the internet. *See* AC ¶¶ 6, 182. Defendants attempt to argue that some further "nexus" to the United States is required under the statute, but this argument has no support in relevant case authority. *See* ECF 63 at 29. Defendants' primary authority is *RJR Nabisco v. European Cmty.*, 579 U.S. 325 (2016), but this case concerned an entirely different statutory scheme—the Racketeering Influenced and Corrupt

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Organizations Act (RICO), 18 U.S.C.S. §§1961-1968. The court there reasoned, under that specific statutory scheme, that the RICO enterprise's conduct occurring abroad must directly involve the United States in some "significant way." 579 U.S. at 344. But the CFAA's definitions, scheme, and jurisprudence are distinct; it is not a RICO hacking statute, and courts have consistently interpreted the commerce requirement as requiring only a connection to the internet. The reason for this is explained by the Ninth Circuit in *Trotter*:

> The Internet is an international network of interconnected computers, . . . and is comparable to 'a sprawling mall offering goods and services. . . . As both the means to engage in commerce and the method by which transactions occur, 'the Internet is an instrumentality and channel of interstate commerce.

Trotter, 478 F.3d at 921 (internal quotations omitted); *see also United States v. Hornaday*, 392 F.3d 1306, 1311 (11th Cir. 2004) ("Congress clearly has the power to regulate the [I]nternet, as it does other instrumentalities and channels of interstate commerce . . . ."); *Ryanair DAC v. Expedia Inc.*, No. C17-1789RSL, 2018 U.S. Dist. LEXIS 131683, at *5–6 (W.D. Wash. Aug. 6, 2018) (noting, in analyzing extraterritoriality, the several ways RICO and the CFAA differ).

For these same reasons, Defendants' argument that the CFAA does not apply to foreign conduct is unavailing. Defendants cite no authority under the CFAA for this proposition, and for good reason: a broad restriction on foreign conduct would be inconsistent with the broad definition of what devices "count" as protected computers under the CFAA. "To do so would make little sense given the conduct the CFAA regulates. That conduct (unauthorized computer access) basically happens simultaneously at the locations of the accessor and the accessed computer, with limitless possible locations that the transmitted data may pass through in between." *Ryanair*, 2018 U.S. Dist. LEXIS 131683, at *6. The definition of "protected computer" is as "clear an indication as possible short of saying 'this law applies abroad.'" *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 448 (N.D.CA 2018) (quoting

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Ryanair, 2018 U.S. Dist. LEXIS 131683, at *2). Alhathloul's iPhone is a protected computer under the CFAA.

B. Alhathloul's Claims are Anchored in Established Facts and Reasonable Inferences.

To prevail on a motion to dismiss for failure to state a claim, the defendant must show "there is no cognizable legal theory to support the claim" or that "the complaint lacks sufficient factual allegations to state a facially plausible claim for relief." *Murphy v. United States*, 2022 U.S. Dist. LEXIS 2299, at *2-3 (D. Or. Jan. 5, 2022) (citing *Shroyer v. New Cingular Wireless Servs.*, Inc., 622 F.3d 1035, 1041 (9th Cir. 2010). Determining the plausibility of a claim requires the court to consider "the entire factual context" of the complaint. *Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (considering "entire factual context to find the plaintiff nudged [her] claim. . . across the line from conceivable to plausible") (internal quotations omitted).

While the Court is required, at the motion to dismiss stage, to accept as true Alhathloul's allegations, what makes this case unique from an ordinary cyber-tort case is the vast set of facts, already admitted by the Individual Defendants, establishing that Defendants operated Karma to hack hundreds of targets. While the DPA makes no mention of *any* individual victim, it identifies the class of victims to which Alhathloul belongs: perceived dissidents of the UAE and Saudi Arabia.

Beyond the vast set of facts in the DPA, the Amended Complaint cites credible reporting from *Reuters* connecting Alhathloul to the conduct Defendants admitted to in the DPA. "Project Raven targeted and hacked Alhathloul," and during the course of this surveillance "assigned her the code name 'Purple Sword.'" AC ¶ 134. *Reuters*' extensive reporting about Project Raven and these Defendants was "based on interviews with whistleblowers who previously worked on Project Raven and an independent review of Project Raven documents." *Id.* ¶ 133. These

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

allegations drawn from *Reuters* are particularly credible when considered in light of the DPA, and together provide a reasonable basis for inferring on information and belief that Defendants committed the alleged violations. *See In re Wet Seal, Inc. Sec. Litig.*, 518 F. Supp. 2d 1148, 1172 (C.D. Cal. 2007) "[N]ewspaper articles should be credited . . . if they are sufficiently particular and detailed to indicate their reliability.") (quoting *In re McKesson HBOC, Inc. Sec. Litig.*, 126 F. Supp. 2d 1248, 1272 (N.D. Cal. 2000)). Defendants neither contest the veracity of this reporting from *Reuters*, nor make any specific mention of it in their Motion to Dismiss.

Alhathloul's "information and belief" allegations are anchored in these established and otherwise credible facts. They are not "speculative," as Defendants characterize them. ECF 63 at 30. As this Circuit recognized, information and belief allegations are "a desirable and essential expedient when matters that are necessary to complete the statement of a claim are not within the knowledge of the plaintiff but he has sufficient data to justify interposing an allegation on the subject." *Bank Melli Iran v. Pahlavi*, 58 F.3d 1406, 1412 (9th Cir. 1995). Indeed, this Circuit will "relax pleading requirements where the relevant facts are known only to the defendants" and a plaintiff need not specifically plead facts to which she cannot be "reasonably expected to have access." *Concha v. London*, 62 F.3d 1493, 1503 (9th Cir. 1995). To the extent the Amended Complaint relies on an "information and belief" allegation to infer the Individual Defendants' culpability, that is necessary because she cannot be "reasonably expected to have access" to information about the inner workings of Project Raven, which by design was a covert operation. *Id.*

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

C. Alhathloul's Claim Meets the Requirements for a CFAA Civil Claim

1. Alhathloul's Physical Injury is Cognizable Under the CFAA.

Defendants wrongly argue that Alhathloul's physical injury is not cognizable under the CFAA because it does not relate to a "technological harm" that must "directly cause physical injury. ECF 63 at 35. This argument fails, for three reasons.

First, Defendants are incorrect that a causal relationship is required. Alhathloul alleges having suffered physical injury because of Defendants' hack and surveillance of her. AC ¶¶ 185, 200–14. The CFAA allows for civil claims when unauthorized access to a protected computer "involves" one of five factors, which includes "physical injury." 18 U.S.C. § 1030(g) ("Any person who suffers damage or loss" may bring a civil action "only if the conduct involves one of the factors set forth" in the statute); § 1030(c)(4)(A)(i)(III) (noting "physical injury" as one factor). Section 1030(g) makes explicit that the relationship between "damage" or "loss" and the "physical injury" is not causal, but merely that damage or loss must "involve" physical injury. To the extent Defendants claim that direct causation is required, *see* ECF 63 at 34–35, their argument is unavailing, and relies on inapposite language in the criminal provisions of the statute.

Second, Defendants appear to collapse "loss" with "physical injury," in order to insist that only technological harms—and not "misuse of information"—are cognizable under the statute. ECF 63 at 34-35. But the CFAA's plain language reflects that physical injury is a distinct type of harm from "loss," rendering inert the invented category of information "misuse." Physical injury, as its ordinary and everyday meaning is understood, does not fit within the definition of "loss"— "any reasonable cost" to a victim. *See* 18 U.S.C. § 1030(e)(11) (listing economic costs).

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

This distinction is also apparent in the statutory structure. Under 18 U.S.C §1030(c)(4)(A)(1), "loss greater than $5,000" and "physical injury" are separate and sufficient predicates for a claim. Interpreting physical injury as synonymous with "loss" would convolute this structure by either treating the physical injury predicate as surplusage (when it results in *more* than $5,000 of harm) or contradicting Congress' intent to set a floor for claims (when a physical injury resulted in *less* than $5,000 of loss). The only reading that gives the physical injury predicate its full effect is to interpret it as distinct from "loss." This view is consistent with *Wofse v. Horn*, in which the court held a plaintiff's "anxiety, panic attacks, insomnia, and internal bleeding" as recognized physical injuries induced by defendant's cyber-attacks. *Wofse v. Horn*, 523 F. Supp. 3d 122, 140 (D. Mass. 2021).

Defendants attempt to stretch *Van Buren*, *Andrews*, and *Fraser* beyond their holding to limit "physical injury" to those relating to a "technological harm," but each case interpreted only the meaning of "loss"—a separate predicate for a civil CFAA claim. *See, e.g.*, *Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021) ("The statutory definitions of 'damage' and 'loss' thus focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data.").

Third, Defendants wrongly argue that the action of Saudi officials was an "independent, intervening cause" that severs liability. But this argument rests on the false premise that causation, rather than involvement, is an operative element in the CFAA analysis. Regardless, not all intervening actions sever liability. Rather, "to qualify as a superseding cause so as to relieve the defendant from liability for the plaintiff's injuries, both the intervening act and the results of that act must not be foreseeable." *Fraser v. Mint Mobile, LLC*, 2022 U.S. Dist. LEXIS 76772, at *9 (N.D. Cal. Apr. 27, 2022); *Ileto v. Glock Inc.*, 349 F.3d 1191, 1209 (9th Cir. 2003)

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

("[A]n intervening act does not amount to a 'superseding cause'. . . if it was reasonably foreseeable"). Regardless, being fact-dependent, this argument is out of place at the motion to dismiss stage.

Court have recognized that acts of a third-party "do not qualify as superseding causes" when they arise from a known or reasonably anticipated threat. *Fraser*, 2022 U.S. Dist. LEXIS 76772, at *9. In *Fraser*, the court found that the defendant's alleged CFAA violation—bypassing the plaintiff's pin verification set up on his mobile account—could be reasonably anticipated to cause the theft of cryptocurrency by a third-party because it made swapping SIM cards easier and "SIM hijacking represent[ed] a national problem." *Id.* (assessing "proximate cause" for "all counts" before assessing whether the theft qualified as a predicate loss).

The intervening actions of Saudi officials should clearly have been reasonably anticipated by Defendants, who carried out surveillance of dissidents at the behest of foreign nations with a pattern of human rights abuse. The Complaint identifies several dissidents who were surveilled by DarkMatter and later arrested; there are likely others. If anything, Alhathloul's physical injury is far more foreseeable than the theft in *Fraser*, where defendants could at least point to intervening acts of a not-yet-identified third-party. Defendants' activity was closely intertwined with the state actors that inflicted her injury: Defendants participated in meetings with government officials who identified the targets for hacking and specifically targeted government dissidents with histories of being previously being arrested, detained, and/or tortured.

2. Defendants' Hack Resulted In Alhathloul's Loss.

Alhathloul suffered loss aggregating at least $5,000 in value, which includes costs incurred due to responding to the hack, conducting a damage assessment, and attempting to restore data." AC ¶ 203. The Amended Complaint alleges that "Alhathloul spent at least 100 hours responding to the hacks committed against her, including communicating with cyber-

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

security experts about the hack, contacting individuals whose information may have been intercepted by Defendants' hack, developing new security protocols, and remaining informed about the latest threats against her digital security. *Id.* ¶ 204. Additionally, Alhathloul was forced to "employ new security measures to protect the confidentiality of her communications, which has impaired her ability to carry out her human rights work." *Id.* ¶ 205.

Defendants do not dispute that these losses fall within the CFAA's definition under 18 U.S.C. § 1030(e)(11), only that they "do not support an inference that Plaintiff incurred $5,000 in costs." ECF 63 at 32. But courts in this Circuit do not require a plaintiff to "allege with detail...when and how and what it was that [plaintiff] allegedly did in response that caused it to incur any loss," when the court can "plausibly infer" that these losses exceed $5,000. *Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1173 (C.D. Cal. 2018). Nor does Alhathloul need to allege she "paid the 'cyber-security experts,'" or anyone for that matter. ECF 63 at 32. The value of the time she spent—*at least* 100 hours—is cognizable loss under this Circuit's precedent and she need not provide detailed accounting to survive a motion to dismiss. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) ("It is undisputed that Facebook employees spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding to" CFAA violations); *Svanaco, Inc. v. Brand*, 417 F. Supp. 3d 1042, 1059 (N.D. Ill. 2019) (at least 85 hours of employee time sufficient to establish loss).

With regard to Alhathloul's further allegations of loss, AC ¶¶ 206–11, the cases cited by Defendants are of limited application when the target of the hack is an individual human rights activist. Most case law on loss, including those cited by Defendants, deals with disputes between consumers, corporate competitors, and employees and employers. *See, e.g., Andrews v. Sirius*

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

XM Radio Inc., 932 F.3d 1253, 1262 (9th Cir. 2019). However, the courts recognized the effect to business operations, loss of customers, and misuse of personal information or trade secrets, that resulted from the hack. *See, e.g., United Fed'n of Churches, LLC v. Johnson*, 2022 WL 1128919, at *8 (W.D. Wash. Apr. 15, 2022) (plaintiff "plausibly alleged that it suffered 'loss' due to the loss of its members" and "the revenue associated with them . . . which in turn was caused by [defendant's] actions").

D. Alhathloul's Conspiracy Claim is Sufficient

The act of state doctrine cannot save Defendants from Alhathloul's conspiracy claim. While the act of state doctrine applies where "the relief sought or the defense interposed would have required a court in the United States to declare invalid the official act of a foreign sovereign performed within its own territory," *W.S. Kirkpatrick & Co. v. Environmental Tectonics Corp., Int'l*, 493 U.S. 400, 405 (1990), here the Court is not presented with a legal issue that requires it to rule on the *validity* of a domestic official act by the UAE. Instead, the question is whether Defendants—non-state actors—violated U.S. law (with regard to Alhathloul's CFAA claims) and the Laws of Nations (with regard to Alhathloul's ATS claims). Indeed, courts routinely consider allegations that implicate the actions of foreign States that violated international law, regardless of the validity of the acts under foreign domestic law. *See, e.g., Doe I v. Cisco Sys., Inc.*, 73 F.4th 700, 728 (9th Cir. 2023) (finding that plaintiffs alleged a plausible claim that "Cisco provided assistance with substantial effect on cognizable violations of international law" by the Chinese Government); *Jane v. Thomas*, 560 F. Supp. 3d 855, 880-83 (E.D. Pa. Sept. 15, 2021) (holding on summary judgment that the defendant, a former Liberian military officer, acted under color of law of Liberia in ordering massacre during civil war that led to violations of the Torture Victim Protection Act and the ATS, and finding the defendant liable); *Kirkpatrick*, 493 U.S. at 406 ("Regardless of what the court's factual findings may suggest as to the legality

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

of the [foreign] contract, its legality is simply not a question to be decided in the present suit, and there is thus no occasion to apply the rule of decision that the act of state doctrine requires.").

III. THE COURT HAS SUBJECT MATTER JURISDICTION OVER THE ALIEN TORT STATUTE CLAIM.

A. The Individual Defendants' U.S.-Connected Conduct Gives Rise to Jurisdiction under the ATS.

Defendants' argument that the Court lacks subject matter jurisdiction over the ATS claim because the claim is impermissibly extraterritorial in nature must be rejected. Alhathloul's claim sufficiently "touch[es] and concern[s] the territory of the United States" so as to "displace the presumption against extraterritorial application." *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124-25 (2013). The outcome is no different under *Nestlé USA, Inc. v. Doe*, because the Amended Complaint alleges "conduct that is relevant to the statute's focus occurred in the United States." 141 S. Ct. 1931, 1934 (2021) ("*Nestlé II*") (quoting *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. 325, 337 (2016)).

As the Ninth Circuit recently explained, an ATS claim is cognizable even where the direct violations were committed abroad. *Doe I v. Cisco Sys., Inc.*, 73 F.4th 700, 736, 739 (9th Cir. 2023) (allegations that defendant took actions domestically which aided and abetted China's direct violations of international law in China overcame presumption against extraterritoriality). "Because the ATS's historical purpose was to provide a remedy for torts committed by U.S. nationals in violation of the law of nations, the identity of an ATS defendant and the claims' overall connections to the United States are relevant" to whether the claims are permissible. *Al Shimari v. CACI Premier Tech., Inc.*, No. 108-CV-827, 2023 WL 5181611, at *23 (E.D. Va. July 31, 2023). Defendants are not helped by observing that Alhathloul was "arrested in the UAE and harmed in the UAE and Saudi Arabia." ECF 63 at 39. *See CACI*, No. 108-CV-827, 2023 WL 5181611, at *10 ("'[I]t is not sufficient merely to say that […] the actual injuries were inflicted

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

abroad,' to find a claim barred by the presumption against extraterritoriality.") (*quoting Al Shimari v. CACI Premier Tech., Inc.*, 758 F.3d 516, 529 (4th Cir. 2014); *Jane W.*, 560 F. Supp. 3d at 877 (E.D. Pa. 2021) (finding *Kiobel*'s "touch and concern" test satisfied even though underlying alleged tortious conduct and injuries were committed abroad).

Alhathloul has alleged that the Individual Defendants aided and abetted and conspired in her persecution. "Aiding and abetting a violation of international law establishes individual or corporate liability for a violation of the law of nations." *Cisco*, 73 F.4th at 737; *see also Mwani v. Bin Laden*, 947 F. Supp. 2d 1, 5 (D.D.C. May 29, 2013) (jurisdiction exists for ATS claims based on alleged conspiracy directed at U.S. interests planned, in part, in the U.S.). Moreover, "conduct within the United States that constitutes aiding and abetting a violation of international law, 'even if other conduct [*i.e.*, the principal's acts] occurred abroad,' is a violation of the law of nations that falls within the 'focus' of the ATS." *Cisco*, 73 F.4th at 737 (brackets in the original (citing *Nestlé II*, 141 S. Ct. at 1936)). Neither *Kiobel* nor *Nestlé* requires that *all* alleged conduct occur in the United States. *See Cisco*, 73 F.4th at 739 (distinguishing *Kiobel* and *Nestlé*, where "all or nearly all the actions that constituted assistance to the principal occurred abroad").

Here, the Amended Complaint alleges that the Individual Defendants, all U.S. persons, engaged in extensive U.S.-connected conduct that is pertinent to aiding and abetting, and conspiracy to commit, the crime against humanity of persecution. This includes, *inter alia*, the Individual Defendants: (1) surveilling Alhathloul's movements and private communications, including with U.S. individuals, and exfiltrating data from her device, including while she was physically present in the United States; (2) developing the UAE's cyber-surveillance program while working for a U.S. company, CyberPoint, using U.S. technology prohibited for export

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

absent a U.S. export license; (3) intentionally accessing and providing U.S. export controlled technology to DarkMatter as part of their specialized work building up the computer exploitation capacity of DarkMatter and its services to UAE agencies; (4) purchasing and customizing exploits to take advantage of vulnerabilities in software and operating systems created by U.S. companies, entering into contract with the U.S. companies to configure the exploits, and transferring over $2 million in funds to U.S. bank accounts to purchase the exploits, *cf. Shimari v. CACI Premier Tech., Inc.*, No. 108CV827LMBJFA, 2023 WL 5181611, at *11 (E.D. Va. July 31, 2023) (domestic conduct relevant to ATS claims included the fact that services were rendered pursuant to a contract that was executed in the United States and provided for payment within the United States); (5) incorporating other U.S. technology into the Karma system, including anonymization services, proxy servers, and computer hardware located or built in the United States, and directing the creation of hundreds of fake accounts with U.S.-connected companies to assist in their cyber-surveillance activities; (6) deploying hacking exploits that targeted Apple's iMessage servers located in the United States, routing their malicious activity through U.S. servers, accessing communications with U.S. persons, and exfiltrating data from U.S.-based devices. For such acts, the Individual Defendants were investigated and prosecuted by the U.S. Department of Justice for violations of U.S. law.

These acts by Individual Defendants, individually and collectively, amount to U.S.-connected conduct that is directly relevant to Alhathloul's claim under the ATS for aiding and abetting and conspiracy to commit the crime against humanity of persecution.

B. The Amended Complaint States a Claim for Persecution as a Crime Against Humanity.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants' argument that "Plaintiff does not allege a recognized tort on which an ATS claim may be based," ECF 63 at 39, and their reference to persecution as "an *alleged* crime against humanity," *Id*. at 38 (emphasis added) also fail. U.S. courts have consistently held that crimes against humanity constitute a violation of the law of nations actionable under the ATS. *Kiobel v. Royal Dutch Petrol. Co.*, 621 F.3d 111, 116–20 (2d Cir. 2010) (recognizing that the ATS provides jurisdiction over crimes against humanity in accord with customary international law), *aff'd*, 569 U.S. 108 (2013); *Doe I v. Cisco Sys., Inc.*, 73 F.4th 700, 715, 746 (9th Cir. 2023) (finding that the plaintiffs plausibly alleged that Cisco aided and abetted violations of international law, which included allegations of crimes against humanity).[7] U.S. courts have also consistently held that persecution that rises to the level of a crime against humanity is actionable under the ATS. *See, e.g., Jane W.*, 560 F. Supp. 3d at 886; *Sexual Minorities Uganda v. Lively*, 960 F. Supp. 2d 304, 316–17 (D. Mass. Aug. 14, 2013) (same); *Wiwa v. Royal Dutch Petrol. Co.*, 626 F. Supp. 2d 377, 384–85 (S.D.N.Y. 2009) (same).

Persecution rises to the level of a crime against humanity when it is an "intentional and severe deprivation of fundamental rights contrary to international law by reason of the identity of the group or collectivity," *Lively*, 960 F. Supp. at 316, that was committed in the context of "a 'widespread or systematic' attack against a civilian population." *Doe v. Qi*, 349 F. Supp. 2d 1258, 1308 (N.D. Cal. 2004). Alhathloul's abduction, unlawful detention, rendition, and torture

[7] *See also Sosa v. Alvarez-Machain*, 542 U.S. 692, 760–62 (2004) (Breyer, J., concurring) (recognizing crimes against humanity as "universally condemned behavior" under international law that is cognizable under the ATS); *Mujica v. Occidental Petrol. Corp.*, 381 F. Supp.2d 1164, 1179-81 (C.D. Cal. 2005) (crimes against humanity create a cause of action under the ATS), *remanded on other grounds*, 564 F.3d 1190 (9th Cir. 2009); *Doe v. Rafael Saravia*, 348 F. Supp. 2d 1112, 1144, 1154–57 (E.D. Cal. 2004) (crimes against humanity meet the standard set forth in *Sosa* for ATS claims); *Mamani v. Berzain*, 654 F.3d 1148, 1152 (11th Cir. 2011) ("[T]his Court has decided that 'crimes against humanity' . . . may give rise to a cause of action under the ATS.").

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

—all intentional and severe deprivations of her fundamental rights—were by reason of her advocacy, which made her a perceived political dissident. AC ¶¶ 43–44. This violation was committed in the context of a widespread or systematic attack.

The Amended Complaint sets forth the widespread nature of the persecution of perceived dissidents, more than adequately alleging a crime against humanity. Alhathloul alleges that the U.S. Department of State Country Reports on the UAE and Saudi Arabia, the United Nations, international human rights organizations, and news outlets reported and documented the widespread nature of the persecution of individuals who criticize the governments of these two countries. *Id.* ¶¶ 34–46, 49, 133–34, 229. For example, the UAE subjected 94 government critics and reform activists to a mass trial, *id.* ¶¶ 41–42, and in 2018, there was a coordinated crackdown on women advocates from Saudi Arabia, including Alhathloul. *Id.* ¶¶ 49, 156–63. Further, Alhathloul alleges that, as part of this widespread attack, Defendants repeatedly targeted perceived dissidents for hacking, including *hundreds* of iPhones. *Id.* ¶¶ 60, 74, 82, 133–34. This is more than sufficient to state a claim for a crime against humanity. *See Qi*, 349 F. Supp. at 1308 ("The concept 'widespread' may be defined as massive, frequent, large-scale action, carried out collectively with considerable seriousness and directed against a multiplicity of victims." (internal citations omitted)).[8]

The Amended Complaint also sufficiently pleads the alternative criterion for a crime against humanity, namely that the attack be "systematic," referring to the "organized nature of the acts of violence and the improbability of their random occurrence." *Presbyterian Church of*

[8] Defendants' argument that Alhathloul's allegations are insufficiently "widespread" because they purportedly "concern only herself and three other individuals" (ECF 63 at 41) mischaracterizes the Amended Complaint. In any event, the single case that Defendants cite, *Mamani v. Berzaín*, 654 F.3d 1148, 1156 (11th Cir. 2011) makes clear that there is no minimum number of victims required to support a finding of a crime against humanity.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Sudan v. Talisman Energy, Inc., 226 F.R.D. 456, 481 (S.D.N.Y. 2005). The Amended Complaint describes the specific and coordinated targeting of individuals perceived by the UAE to be dissidents—including Alhathloul—and thus plainly alleges that her mistreatment was "systematic" in the sense that it was not accidental or random, but part of an organized pattern of abuse orchestrated against perceived dissidents, such as herself. AC ¶¶ 14–46. Further, as part of this systematic attack, the Amended Complaint alleges that Defendants engineered sophisticated exploits and followed a protocol to target perceived dissidents for hacking, *Id.* ¶¶ 65–71, 87–110, and that the UAE had a cooperation agreement with Saudi Arabia so that the two countries could assist each other in the persecution of perceived dissidents. *Id.* ¶¶ 47–54.

Lastly, the Amended Complaint provides a detailed account of the key roles that the Individual Defendants knowingly played to facilitate the UAE's widespread and systematic campaign to target perceived dissidents, including Alhathloul, through their development, maintenance, deployment and operation of Project Raven. AC ¶¶ 65–72, 83–110, 133–34, 231. *Cf. Cisco*, 73 F.4th at 726 ("[A]n actor may have a substantial effect on the perpetration of international law violations by supplying computer hardware, software, or technological support that enhances the capacity of the principal to coordinate and facilitate operations in which crimes are committed.").

C. Defendants' Reliance on Authority That Applies Foreign Sovereign Immunity Is Misplaced.

Defendants present an implicit foreign sovereignty argument with regard to Alhathloul's ATS claims, relying on *Broidy Cap. Mgmt., LLC v. State of Qatar*, 982 F.3d 582, 592 (9th Cir. 2020) ("*Broidy I*"). ECF 63 at 34. But *Broidy I* involved a suit brought against the State of Qatar, requiring the application of the Foreign Sovereign Immunities Act (FSIA). The FSIA

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

provides the legal framework conferring immunity on foreign states and their agencies or instrumentalities unless specific exceptions apply. 28 U.S.C.A. § 1603. Because there was "no dispute" that Qatar qualifies as a foreign state, the Ninth Circuit held that Qatar was immune from jurisdiction. *Broidy I*, 982 F.3d at 590.

The Defendants in this case are neither a foreign state nor an agency or instrumentality of a foreign state, and therefore cannot assert immunity pursuant to the FSIA. *See WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 17 F.4th 930, 933 (9th Cir. 2021), *cert. denied*, 143 S. Ct. 562 (2023). The Individual Defendants are not foreign officials, and even if they were, they would not be immune under the FSIA. *See Samantar*, 560 U.S. at 316, 325 (the FSIA's definition of a "foreign state" does not include foreign officials acting on the state's behalf, and "agency or instrumentality" does not include natural persons). To the extent the Individual Defendants may claim foreign official immunity under the common law, their claim also fails. *See Samantar*, 560 U.S. at 311-312. The circumstances of the Individual Defendants are insufficient for a finding of common law residual foreign official immunity. *See Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789, 800 (D.C. Cir. 2021) ("*Broidy II*") (In a case arising out of the same facts as *Broidy I*, individual defendants who assisted Qatar in hacking and disseminating private documents as contractors providing services did not satisfy requirements for common law foreign official immunity.)

CONCLUSION

For the forgoing reasons, Defendants' Motion to Dismiss should be denied.

BOISE MATTHEWS DONEGAN LLP
805 S.W. Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Certificate of Compliance

This brief complies with the applicable word-count limitation under L.R. 7-2(b), with leave granted by the Court to exceed the page or word limitation by no more than ten pages or 2,000 words, (ECF 69) because it contains 12,988 words, including headings, footnotes, and quotations, but excluding the caption, table of contents, table of cases and authorities, signature block, exhibits, and certificate of counsel.

Dated: September 19, 2023 /s Christopher E. Hart

BOISE MATTHEWS DONEGAN LLP
Bridget M. Donegan
OSB No. 103753
805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

FOLEY HOAG LLP
Christopher E. Hart
MA BBO No. 625031
Anthony D. Mirenda
MA BBO No. 550587
Andrew Loewenstein
MA BBO No. 648074
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1000
chart@foleyhoag.com
adm@foleyhoag.com
aloewenstein@foleyhoag.com

ELECTRONIC FRONTIER FOUNDATION
David Greene
CA Bar No. 160107
Sophia Cope
CA Bar No. 233428
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
davidg@eff.org
sophia@eff.org

CENTER FOR JUSTICE AND ACCOUNTABILITY
Daniel McLaughlin
CA Bar No. 315326
Claret Vargas
MA BBO No. 679565
Carmen Cheung Ka Man
NY Bar No. 4132882
268 Bush St. #3432
San Francisco, CA 94104
(415) 544-0444
dmclaughlin@cja.org
cvargas@cja.org
ccheung@cja.org

Attorneys for Plaintiff Loujain Hathloul Alhathloul